JOURNAL OF NUMBER THEORY 62, 368–374 (1997)
ARTICLE NO. NT972053

Representation of Integers by Positive Definite Binary Hermitian Lattices over Imaginary Quadratic Fields

A. G. Earnest* and Azar Khosravani†

Department of Mathematics, Southern Illinois University at Carbondale, Carbondale, Illinois 62901-4408

Communicated by J. S. Hsia

Received October 3, 1995; revised February 6, 1996

Let L be a positive definite binary integral hermitian lattice over an imaginary

INTRODUCTION

The local representation theory for hermitian lattices is well understood, in light of the work of Johnson [6] (in the non-split case) and Gerstein [4] (in the split case). Consequently, to answer the fundamental question of what integers are globally represented by such a lattice L, it remains to examine the set of integers which are represented by all localizations of L, but not globally by L. To facilitate the discussion here, we define $E(L)$ to be the number (possibly infinite) of such "exceptional" integers. Our main goal will be to prove the result stated in the abstract; this appears as Theorem 2.2. This result can be viewed as complementary to a recent theorem of Hsia and Prieto-Cox [5] which shows, in particular, that $E(L)$ is bounded from above for positive definite hermitian lattices of rank exceeding 2. Indeed, that result is obtained as a special case of quite general results that apply to the representation of lattices by hermitian lattices in general CM-extensions.

Watson [9] obtained the corresponding theorem in the theory of integral quadratic forms. He proved that for positive definite ternary quadratic forms f, the number of integers represented everywhere locally by f, but not globally by f, is asymptotically bounded from below by a power of the

* Research supported in part by a grant from the National Security Agency.

† Current address: Department of Mathematics, University of Wisconsin, Oshkosh, Oshkosh, WI 54901-8631.

0022-314X/97 $25.00

discriminant. Indeed, the inspiration for the methods used in the present paper stems from that source. A slightly modified proof for the growth of $E(L)$ with the discriminant, emphasizing the role of the successive minima, was given by the first author in [3]. One consequence of this growth is that there exist only finitely many classes of positive definite ternary quadratic forms which are regular, in the sense of Dickson [1]; that is, which represent all integers represented by their genus. This finiteness does not extend to quaternary quadratic forms, as shown by an example given in [3]. The study of higher dimensional analogues of this type of regularity for quadratic lattices was initiated in [2].

As the ring of integers of an imaginary quadratic field is not generally a principal ideal domain, the lattices to be considered in the present context need not be free. Thus, we need to argue the growth of the exceptional set in terms of the volume, rather than the discriminant, of the lattices. The strategy will be to obtain asymptotic upper bounds on the magnitudes of the successive minima of lattices having exceptional set of a specified size. From our main result will follow the finiteness of the number of classes of positive definite binary hermitian lattices which are regular in the sense analogous to the use of that term mentioned above for quadratic forms. As there exist universal hermitian lattices over some imaginary quadratic fields, this finiteness does not extend to ternary hermitian lattices.

1. PRELIMINARIES

Throughout this paper we will adopt the terminology and notation for lattices as in O'Meara's book [7]. For background results and terminology specific to the hermitian case, the reader is referred to the papers [4], [6] and [8].

Let $E = \mathbf{Q}(\sqrt{m})$, where m is a squarefree negative integer, and let $\mathcal{O}$ be the ring of algebraic integers of E. Let (V, H) be a nondegenerate hermitian space over E (that is, $H: V \times V \to E$ is linear in the first variable and conjugate linear in the second), and let L be an $\mathcal{O}$-lattice on V. For such a lattice L, there exist $x_1, ..., x_n$ in V and fractional $\mathcal{O}$-ideals $\mathcal{A}_1, ..., \mathcal{A}_n$ such that $L = \mathcal{A}_1 x_1 + \mathcal{A}_2 x_2 + \cdots + \mathcal{A}_n x_n$. The *volume* vL of L is defined to be the fractional $\mathcal{O}$-ideal

$$vL = (\mathcal{A}_1 \overline{\mathcal{A}_1})(\mathcal{A}_2 \overline{\mathcal{A}_2}) \cdots (\mathcal{A}_n \overline{\mathcal{A}_n}) \det(x_1, x_2, ..., x_n).$$

Note that each of the $\mathcal{A}_i$'s can be written as a product of integral powers of prime ideals of $\mathcal{O}$. For any prime ideal P of $\mathcal{O}$, let p be the rational prime such that P lies over $p\mathbf{Z}$. Then we have

$$P\overline{P} = \begin{cases} p^2\mathcal{O}, & \text{if } p \text{ is inert in } E \\ p\mathcal{O}, & \text{otherwise.} \end{cases}$$

Consequently, there is a unique positive rational number δ_L with the property that $vL = \delta_L \mathcal{O}$.

For a rational number a, we say that a is represented by L, denoted $a \to L$, if there exists a vector x in L such that $H(x) = a$, where $H(x) := H(x, x)$. All lattices L considered in the remainder of the paper will be positive definite; i.e., $H(x) > 0$ holds for all nonzero $x \in L$. The norm of L, denoted nL, is the $\mathcal{O}$-ideal generated by $\{H(x) \mid x \in L\}$. We will assume throughout that L is integer-valued, in the sense that $nL \subseteq \mathcal{O}$. Moreover, we will refer to the lattice L as primitive if equality holds.

The successive minima of L are defined as in the case of quadratic lattices in [2; Definition 2.1]. The inequality for the product of the successive minima in the following proposition, which is the hermitian analogue of [2; Proposition 2.3], is fundamental for the proof of our theorem.

PROPOSITION 1.1. *Let L be a positive definite hermitian lattice of volume $\delta_L \mathcal{O}$ over $\mathcal{O}$ with successive minima $\mu_1, \mu_2, ..., \mu_n$, where δ_L is a positive rational number. Then*

$$\delta_L \leqslant \mu_1 \mu_2 \cdots \mu_n.$$

Proof. Consider first the case where L is free. Let $\mathbf{B}_H = \{v_1, ..., v_n\}$ be a basis for L, let $M = (H(v_i, v_j))$, and $D = \det M$; so $\delta_L = D$. Let $m_1, ..., m_n$ be linearly independent vectors of L such that $H(m_i) = \mu_i$, and let x_i be the coordinate vector (written as a column vector) for m_i with respect to $\mathbf{B}_H$. Let $X \in M_n(\mathcal{O})$ be the matrix with columns $x_1, ..., x_n$. Since M is positive definite hermitian, the matrix $A = X^* M X$ is positive definite hermitian, where X^* denotes the conjugate transpose. It is well known that there exists a nonsingular upper triangular matrix P such that $A = P^* P$. The i-th diagonal entry of A is

$$\mu_i = H(m_i) = \sum_{j=1}^{i} \overline{p_{ji}}\, p_{ji} \geqslant \overline{p_{ii}}\, p_{ii}.$$

Thus

$$\prod_{i=1}^{n} \mu_i \geqslant \prod_{i=1}^{n} \overline{p_{ii}}\, p_{ii} = (\det(P^*))(\det(P)) = N(\det(X))\, D \geqslant D$$

since $N(\det X)$ is a positive integer.

Consider now the general case. As before, let $m_1, m_2, ..., m_n$ be linearly independent vectors in L with $H(m_i) = \mu_i$. Consider the sublattice $L' = \mathcal{O}m_1 + \mathcal{O}m_2 + \cdots + \mathcal{O}m_n$ of L. Note that L' has the same successive minima as L. Since $L' \subseteq L$, the volume of L' is contained in the volume of L; i.e.,

$vL' \subseteq vL$. So $\delta_L \leqslant \delta_{L'}$ for the positive rational numbers $\delta_L, \delta_{L'}$ such that $vL = \delta_L \mathcal{O}$, $vL' = \delta_{L'} \mathcal{O}$. By applying the argument above to L', we conclude that $\delta_L \leqslant \mu_1 \mu_2 \cdots \mu_n$. ∎

2. MAIN RESULTS

For the remainder of this paper, L will always denote a primitive binary hermitian lattice over the ring of integers $\mathcal{O}$ of an imaginary quadratic field $E = \mathbf{Q}(\sqrt{m})$, where m is a squarefree negative integer. The following notation will remain in effect throughout this section. Let δ_L denote the positive rational number for which $vL = \delta_L \mathcal{O}$, and let $2, p_1, ..., p_{r-2}$ be the list consisting of all prime divisors of $2m$ and all primes p for which δ_L is not a p-adic unit, let $b = 2p_1 \cdots p_{r-2}$ and $T = \{2, p_1, ..., p_{r-2}\}$. For $i = 1, ..., r-2$, we define $\Psi_i(*)$ to be the character modulo p_i defined by the Legendre symbol $(*/p_i)$. Let $\Psi_{r-1}(*)$ and $\Psi_r(*)$ be the characters modulo 8 defined by the Jacobi symbols $(-1/*)$ and $(2/*)$, respectively.

LEMMA 2.1. *Let a be a positive integer represented by L such that $\gcd(a, b) = 1$. Suppose that c is a positive integer such that $\Psi_i(x) = \Psi_i(a)$ for all $i = 1, ..., r$. Then c is represented by L_p for all primes p.*

Proof. For $p \notin T$, L_p is unimodular. Then $c \to L_p$ follows from [4; 1.8] if p is split, [6; Theorem 4.4] if $E_p/\mathbf{Q}_p$ is an unramified quadratic extension, or [6; Theorem 5.5] if $E_p/\mathbf{Q}_p$ is a ramified quadratic extension. For $p \in T$, both a and c are p-adic units. The character conditions then imply that $c = at^2$ for some p-adic unit t. Since $a \to L_p$, we have also $c \to L_p$. Hence, $c \to L_p$ for all primes p. ∎

We are now ready to prove our main result. In what follows, a statement of the type "$A \ll B^{t+\varepsilon}$" will mean "for any $\varepsilon > 0$, $A \ll B^{t+\varepsilon}$, where the implied constant depends only on ε". The symbol ε will be used in a generic sense; that is, we will not assume that ε has the same value at every occurrence.

THEOREM 2.2. *For primitive positive definite binary hermitian lattices L with volume $\delta_L \mathcal{O}$ over the ring of integers $\mathcal{O}$ of a fixed imaginary quadratic field $\mathbf{Q}(\sqrt{m})$, $E(L)$ tends to ∞ as δ_L tends to ∞.*

Proof. Let k be a positive integer and assume that L is a lattice satisfying the hypotheses of the theorem with $E(L) = k$. We seek first to asymptotically bound from above the size of the minimum μ_1 of L.

Since $nL = \mathcal{O}$, L represents an integer a such that $\gcd(a, b) = 1$. By a straightforward extension of [2; Corollary 3.3], there exists a positive

integer λ_k such that more than k positive integers n not exceeding λ_k satisfy $\psi_i(n) = \Psi_i(a)$ for all $i = 1, ..., r$ where

$$\lambda_k \ll (4b)^{3/8+\varepsilon} \ll b^{3/8+\varepsilon} \ll \delta_L^{3/8+\varepsilon}.$$

For all such n, n is represented by L_p for all primes p by Lemma 2.1. Since $E(L) = k$, at least one of these integers n must be represented by L. Hence,

$$\mu_1 \ll \delta_L^{3/8+\varepsilon}.$$

To estimate the magnitude of the second minimum μ_2 of L, we begin by estimating the size of a certain prime q. Let q be the smallest positive integer (necessarily a prime) such that $\gcd(q, 2\mu_1\delta_L) = 1$ and $(m/q) = -1$. Applying [2; Corollary 3.3] with character $(m/*)$ of modulus $8m$, specified value -1 and Δ equal to the product of the prime divisors of $\mu_1\delta_L$ which do not divide $2m$, we obtain

$$q \ll m^{3/8+\varepsilon}(\mu_1\delta_L)^{\varepsilon}.$$

Combining this with the above and noting that m is constant gives

$$q \ll \delta_L^{\varepsilon}.$$

We claim that no multiple of q, denoted θq, with $\gcd(\theta, q) = 1$, belongs to the set $\{\mu_1 N(\alpha) \mid \alpha \in \mathbf{Q}(\sqrt{m})\}$. Otherwise the two binary quadratic spaces $[\mu_1, -m\mu_1]$ and $[\theta q, -\theta qm]$ over $\mathbf{Q}$ must be equivalent and consequently have the same q-adic Hasse invariants; i.e., $Sq([\theta q, -\theta qm]) = S_q([\mu_1, -\mu_1 m])$. As m and μ_1 are q-adic units

$$S_q([\mu_1, -\mu_1 m]) = (\mu_1, -\mu_1 m)_q = 1.$$

On the other hand,

$$S_q([\theta q, \theta qm]) = (\theta q, -\theta qm)_q = (\theta q, m)_q = (\theta, m)_q (q, m)_q = (m/q) = -1$$

since both m and θ are q-adic units. This proves the claim.

Now suppose that t is a positive integer such that

$$\text{(i)} \quad \gcd(t, 2\delta_L mq) = 1$$

and

$$\text{(ii)} \quad \Psi_i(t) = \Psi_i(a)\,\Psi_i(q) \qquad \text{for all} \quad i = 1, ..., r.$$

Then $\Psi_i(tq) = \Psi_i(t)\,\Psi_i(q) = \Psi_i(a)\,\Psi_i(q)\,\Psi_i(q) = \Psi_i(a)$. By Lemma 2.1, $tq \to L_p$ for all p. By the above argument, $tq \notin \{\mu_1 N(\alpha) \mid \alpha \in E\}$. This latter condition guarantees that x_1, x_2 are linearly independent for any $x_1, x_2 \in L$ such that $H(x_1) = \mu_1$ and $H(x_2) = tq$.

Applying [2; Corollary 3.3] with characters $\Psi_1, ..., \Psi_r$, specified values $\eta_i = \Psi_i(q)\,\Psi_i(a)$, and $\Delta = q$, there exist more than k positive integers t such that $tq \to L_p$ for all p, and which do not exceed

$$\lambda_k \ll (4b)^{3/8+\varepsilon} q^{\varepsilon}.$$

At least one of these integers tq must be represented by L; hence

$$\mu_2 \ll (4b)^{3/8+\varepsilon} q^{\varepsilon}.$$

Combining with the above estimate for q gives

$$\mu_2 \ll \delta_L^{3/8+\varepsilon}.$$

Thus we obtain an asymptotic bound for the product of the successive minima:

$$\mu_1\mu_2 \ll \delta_L^{3/8+\varepsilon}\,\delta_L^{3/8+\varepsilon}.$$

It follows that

$$\mu_1\mu_2 < K\delta_L^{6/8+\varepsilon},$$

where K is a constant. By Proposition 1.1 we have $\delta_L \leqslant \mu_1\mu_2 < K\delta_L^{3/4+\varepsilon}$. Since this inequality is satisfied for only finitely many values of δ_L and there are only finitely many lattices over $\mathcal{O}$ of a given volume [7; 103:4], there are only finitely many lattices over $\mathcal{O}$ with $E(L) = k$. This completes the proof.

A hermitian lattice L is called regular if L represents every integer that is represented by its genus. In other words, L is regular if $E(L) = 0$. The following result is a direct consequence of Theorem 2.2.

COROLLARY 2.3. *There are only finitely many classes of primitive regular positive definite hermitian lattices over the ring of integers $\mathcal{O}$ of a fixed imaginary quadratic field $\mathbf{Q}(\sqrt{m})$.*

REFERENCES

1. L. E. Dickson, Ternary quadratic forms and congruences, *Ann. of Math.* **28** (1927), 333–341.
2. A. G. Earnest, The representation of binary quadratic forms by positive definite quaternary quadratic forms, *Trans. Amer. Math. Soc.* **345** (1994), 853–863.

3. A. G. Earnest, An application of character sum inequalities to quadratic forms, *in* "Number Theory" (K. Dilcher, Ed.), Canadian Math. Soc. Conf. Proc., Vol. 15, pp. 155–158, Canadian Math. Society, 1995.
4. L. J. Gerstein, Integral decomposition of Hermitian forms, *Amer. J. Math.* **92** (1970), 398–418.
5. J. S. Hsia and J. P. Prieto-Cox, Representation of positive definite hermitian forms with approximation and primitive properties, *J. Number Theory* **47** (1994), 175–189.
6. A. A. Johnson, Integral representations of hermitian forms over local fields, *J. Reine Angew. Math.* **229** (1968), 57–80.
7. O. T. O'Meara, "Introduction to Quadratic Forms," Springer-Verlag, Berlin, 1963.
8. G. Shimura, Arithmetic of unitary groups, *Ann. of Math.* **79** (1964), 369–409.
9. G. L. Watson, The representation of integers by positive definite ternary quadratic forms, *Mathematika* **1** (1954), 104–110.